15(L)

TOP SECRET 'U' TICOM/1-20

INTERROGATION OF SONDERFUEHRER DR. FRICKE OF OKW/CHI

(FORMERLY OF OKH/CHI).

The reports attached are of the first and second detailed interrogations of Sonderfeuhrer Dr. FRICKE at the OKM Signals School, FLENSBURG on 16th and 17th June,1945.

Annexed to this report is the translation of seven pages of typescript offered to the interrogators by Dr. FRICKE, being part of some sets of questions submitted to Chef WNV by unknown persons (presumably an Allied authority). These particular questions were passed on to FRICKE by WNV for preparation of answers. Question 5 of the second list and its answer are not FRICKE's.

The initial interrogation of Dr. FRICKE, together with Oberst KETTLER and Reg. Rat. Dr. HUETTENHAIN, all of OKW/Chi, and Oblt. SCHUBERT of OKH, were carried out in the SCHLOSS GLUCKSBURG on 15th June, 1945. A report on this interrogation is being issued separately.

TICOM
28th June, 1945.

Copy No. 11
No. of pages.

DISTRIBUTION

British
1. Director
2. D.D.3.
3. D.D.4.
4. D.D.(N.S.)
5. D.D.(M.W.)
6. D.D.(A.S.)
7-8. A.D.(C.C.R) (2)
9. Col. Leatham

Ticom
10. Chairman.
11-12. S.A.C. (2)
13. Cdr. Bacon.
14. Cdr. Mackenzie.
15. Cdr. Tandy.
16. Lt. Col. Johnson.
17. Major Seaman.
18. Lt. Eachus
19. Lt. Vance.
20. Capt. Cowan.
21. Lt. Fehl.
22-24. Ticom Files (3)

U.S.
25-26. OP 20-G (2)
(via Lt. Pendergrass)
27. G-2 (via Lt. Col. Hilles)
28-29. S.S.A. (2)
(via Major Seaman)
30. Director, S.I.D. ETOUSA
(via Lt. Col. Johnson)

Additional
Major G.W. Morgan
A.D. (Mch).
Lt. Cdr. [illegible]

Interrogation of Sonderfuehrer Dr. Fricke, held at the Signal School, Flensburg.

First Interrogation. 16 June 1945, P.M. Present: Major Seaman, AUS; Capt. Royffe, IC; Lt. Kirby, AUS

1. Dr. Fricke was asked to give a chronological account of his career. He stated that he had been an astronomer at the Hamburg observatory. In 1934 he studied astronomy, mathematics and physics in Berlin. In 1935 he published his first astronomical works. These were critiques of studies made at the Mt Wilson observatories by Wilson and Hubble on the distribution of spiral nebulae. Later he studied cosmological problems under Prof. Milne in England. He published studies on the distribution and velocities of spiral nebulae in the German Astrophysical Journal. In 1939 he took his doctorate at the Göttingen observatory on the dynamics of stellar systems. He had obtained a scholarship at Edinburgh University which he was to have begun on 1 October 1939. He had got this scholarship through the good offices of Dr. MacVittie. On 1 May 1940 he went to work at the Hamburg observatory, but was drafted into the Nachrichtentruppe during that year. On 15 May 1941 he was posted to OKH/Chi. At that time he knew nothing of cryptography. The director of the Hamburg observatory, Prof. HECKMANN, kept trying to get him back, to work on problems he had been occupied with before he was drafted, and which were related to the war effort: tables of air and ship navigation, and aerodynamic problems for airplane speeds over 1300 km per hr, as well as for rockets with speeds upwards of 3000 km per hr. These were purely mathematical problems involving the solution of differential equations which were farmed out to astronomical and mathematical institutions.

2. At OKW/Chi he studied German cipher methods and devised new ones. These were military systems only. It was known that the single step double box system TS 42 was breakable; they set out to solve the double step system NS 42 ((double playfair)) and after a year's work found a solution.

The head of his section at OKH/Chi at this time was Dr. PIETSCH, who had about eight mathematicians under him. Fricke remained there until 1 November 1944, at which time OKH was forbidden to devise new systems, this function being restricted to OKW/Chi. His section was therefore transferred to OKW/Chi.

4. Returning to the subject of his work at OKH, Fricke stated that he worked for a year on the solution of German systems, then set about the task of developing new ones. He had made some study of enigma solution, but Dr. [illegible] was much better informed on this subject. In 1941 they criticised the [illegible] indicators and these were eliminated. They did not develop a solution [illegible] them, but saw that it could be done.

. In 1941 he developed the Schlüsseltafel, or enciphering tables for 3/letter field codes. Before that they had been used without encipherment. Daily

6. Then he developed the Rasterschluessel. A study was made of the English cipher raster ((Cysquare)), and it was found to be very good. He doesn't know whether it was ever broken, but thinks not. However they thought that if the Gefmans used it in exactly the same form it would be broken because their messages were longer.

He said he would like to know whether any rasters were ever solved, because although he was convinced that if properly used it was unbreakable, they never knew whether mistakes were made which rendered it soluble. We replied that it would be impossible for us to give him an answer. He said they always had wanted to work on their own traffic just as they would do on foreign material, but were never given the opportunity. They never knew how the Army actually used the systems which they put out and they never saw any real traffic. When they asked for real traffic, they were given specially prepared messages, one of which read: "We are standing in Berlin and see the Polish infantry coming down the Frankfurter Allee". They often reflected that the work on Russian systems showed that those systems were secure if properly used, but if the cryptographers in Moscow could only see how they were used they would be very unhappy.

7. Whenever the Army was asked to change a system, there was a storm of protest. It was not they but the HNV (Heeresnachrichtenverbindung) staff which made the decision on methods to be used. The results depended on whether the officer at HNV at the time happened to know anything about cryptology. He usually did not. In 1942 all hand systems were solvable. When the HNV was told this, the reply was that Germany had won all her battles so far, using these systems, and there was no need to overload the troops with new methods.

8. Dr. Fricke then proposed to speak of recent improvements in the Enigma machine:

(a) Stecker Uhr. This was a small device to change the plugging. It gave 40 variations. They knew that the strength of the machine lay in the stecker and therefore wished to divide the traffic load per stecker by 40. The machine was used only by the Luftwaffe, which had only 1000 or so machines for higher echelons.

(b) Because of the uniform motion of the enigma, they considered that if messages of 600 or 700 letters were sent, they could be broken. If the instructions on maximum message length were followed, they knew everything would be all right, but they felt sure that their instructions were not followed. So they developed a new wheel with 26 notches which could be filled in as desired. These were called Lüchenfüllerwalze. They wished to avoid certain numbers of notches per wheel, and particularly consecutive notches, for with the latter it was difficult to predict the cycle except in special cases. Consequently they ordered that wheels should be used with one, five, seven, or nine notches only, and never with consecutive notches. Some of these wheels were actually built in Berlin by HEIMSOETH & RINCKE, who built the enigma. They were to be produced in numbers by this form and by Siemens Halske, and were expected to be ready on 1 May 1945. They were not ready, however.

(c) Pluggable reflector. This was used only on some Luftwaffe traffic. It was not considered important, as the stecker is the real safeguard.

(d) Gerät 39. This machine was to have embodied all their enigma experience. It would print both cipher and clear on tapes. It contained

9. They saw that the Americans had improved the Hagelin by introducing

This machine was used only by the Reichswetterdienst, which had a 10-digit machine. As messages in depth are still soluble, they recently sought a means of changing the alphabet on the printing wheel.

10. The chief teleprinter cipher machines were the Siemens SFM T52c, d and e. They knew that models a and b, as well as c, could be broken, and this is why they undertook to improve the machines. All of these machines performed first a substitution, then a transposition, of the teleprinter-code letters. There were ten wheels with fixed patterns. These activated five relays which performed the substitution, and five others which performed the transposition, but these were not directly connected. The relations between them were varied by means of plugs.

((Comment: [illegible] notes that there are in fact only four [illegible] which are not [illegible].))

11. The Army always said that no teleprinter machine could be solved. When OKW/Chi proved that the 52c could be solved on 10,000 letters of text (this was done by Hüttenhain and he could give the details), the Army said well, nobody taps our cables. This was probably false too, as they had reports of the Swedes reading t/p traffic, on the 52a used by their military attache in Stockholm. When these reports came in they were astounded because they could not break it themselves and doubted that anyone else could. They asked themselves whether the Swedes would really attempt to tap such difficult traffic, and if they did, how they could possibly have broken it. However they knew that all of their 52c and 52d keys had been captured in August/September 1944, and wondered if the Swedes had somehow got hold of these keys.

12. He went on to speak about the plugging.

13. Another type of t/p machine they had observed in an American prototype

14. The Auswärtiges Amt used the T52 series of teleprinter cipher machines. The Luftwaffe had intended to drop the T52c on 1 May 1945.

15. He never saw the American machine referred to above. The Heereswaffenamt told them that we had once used this machine and then dropped it and they wondered why, inasmuch as we used the Hagelin, a simpler and well-known machine. In response to a question as to how the HWA knew about this machine, he said he did not know, but thought perhaps it was used commercially, as the Reichspost was said to have known about it too.

16. He then spoke about the FS Zusätze 40 and 42. These had recently been used only by the army. They performed a substitution only, and were used only on W/T.

machines were made by Lorenz in Berlin. They had intended to improve the SZ 42 and in fact had under construction a 42c. He did not make the plans for this. It was done by Dr LIEBKNECHT, the expert on teleprinter cipher machines at the Heereswaffenamt. The machine would have had much improved synchronization, accomplished by means of quartz clocks, and many cryptographic changes. He referred us to Hüttenhain for these, as the latter had charge of it.

(6)

17. At the close of this interrogation, Dr. Fricke said he hoped he would be allowed to return to Hamburg observatory where he could once more engage in useful work. He has a job open to him there.

Second interrogation. 17 June 1945, P.W. Oberlt Schubert was in the room but took no part in the discussion.

Present: - Major Morgan I.C., Major Seaman A.U.S., Capt. Rayffe I.C.,
Lieut. Kirby A.U.S.

18. The question was raised of the place of the Heereswaffenamt in the Wehrmacht organization. Dr. Fricke stated that it was a subdivision of the Oberbefehl des Ersatzheeres ((reserve Hq)) which had charge of the development of equipment for all arms and services. WA Prüf 7 developed Signal Corps equipment, and Gruppe IV of this developed cipher machines. The head of the group was Oberstlt. MAECHTER. The HWA itself was on the same level as the Allgemeines Heeresamt ((Inspector General's office)), which had subdivisions numbered like the HWA for the inspection of the various arms and services. ((The last bit contributed by Oberlt. SCHUBERT)). Fricke did not know anything about the other HWA departments.

19. He was asked the whereabouts of Dr. LIEBKNECHT of HWA, and replied that he last heard of him at Planken near Magdeburg, where the Versuchsanstalt des Heereswaffenamts had been moved from Berlin.

20. Asked about the Main Reich Security office, which had been mentioned elsewhere in connection with cipher security ((possibly a misapprehension)), Fricke knew nothing about it. He referred to the RSHA generally, however, and said it had the same systems as the Army, at least the T52 machines and the enigma. He knew Oberinspektor Menzer, who had a development and security group like Fricke's, but who worked independently of him. Menzer made up systems for the RSHA, the Reichsbank, the Postoffice, and other governmental agencies. Menzer had been in OKW/Chi long before Fricke came and at one time had developed methods for the army. They worked in the same building. Menzer had recently been working on the development of two cipher devices, which he proceeded to describe.

21. The first was called Schlüsselkasten. It was under construction by the WANDERER typewriter firm at Chemnitz.

This device weighed 800 grams.

22. The second device was similar but only the size of a can of shoe-polish. The three wheels were mounted on the same axis, in the same plane as the box cover.

This device was called Schlüsselscheibe. The development of the two was not ended at the close of the war. If they had proved secure, the army had intended to use them in place of its hand systems.

23. ((Previous information indicated, besides Fricke and Menzer's subsections of OKW/Chi Gruppe II, a subsection IIc dealing with cipher security. Fricke was asked about this section)). Section IIc was not formed until the reorganization of 1 November 1944. Its head, a Captain of Panzer troops whose name Fricke has

has/
forgotten, did not arrive until January or February 1945. He had no knowledge of cryptography, and had only a small staff from the Luftwaffe. The section accomplished nothing.

24. He was asked whether his section had developed a mathematical general or special theory of cipher machine cycles. He said that it had not. One must have mathematical training for cryptography, but the mathematical tools employed are elementary, for example theory of probability ((!)). Asked whether they had computed the period of SG 41, he said no. He only worked on the machine slightly, enough to see that the conversion of key into its complement was needed. Others worked on other security features of it. In fact, his section did not develop the machine; Menzer did most of it.

25. He said he had some things to add to the previous day's statements. He had neglected to mention weather systems. There was the Barbarasschl"ssel, a a terrible system used not for synoptics, but for reporting weather constants such as wind velocity at various heights: 100, 200, ... 10,000 meters, for the information of anti-aircraft and artillery. It employed an additive with as many as 100 messages in depth. ~~Chef HNV had ordered it into as many as 100 messages in depth.~~ Chef HNV had ordered it into use in 1939 and OKW/Chi never heard of it until 1944. In a day or two "I saw that it was clear text". He added that an enemy might think these messages uhimportant, but in fact they were extremely valuable and could even be used by enemy bombers for calculating the trajectory of their bombs. A new system had therefore been devised, and instructions printed, but it had not gone into effect. He was required to use an additive table of the same size, to save paper, so he made an eight-position grille, of which several were/to be used on the additive tableiduring the month.

26. The synoptic systems used by the Reichswetterdienst were also poor. It was therefore intended to introduce the SG 41, on which cribs would be of no use. First they planned to use the machine in letter form, but later they decided to have a digit model.

27. With regard to the instructions for making up emergency enigma keys which he had given us, he wished to say that these were issued recently when lack of transportation made it impossible to distribute new keys.

28. With regard to the tapping of their 52d lines, he added that there had been only a few evidences of this. Most came from Oberpostrat HALDER in the office of the mil. att. Stockholm, whose latest report thereof was received in September 1944. In consequence they put their newest and most secure machines, the T52e and T43 onto this line. This same HALDER, however did a very foolish thing himself which OKW/Chi was at a loss to understand: he asked Oslo to send him T52 keys in clear.

29. With regard to SZ 40 and 42, he said he had asked that they be used only on Linieverkehr and not Netzverkehr, because two messages in depth could be read.

30. We then asked him to tell what he knew of German ciphony. He said no true encipherment systems were actually in use. Methods used were breakable, and amounted only to Erschwerungsger"at ((lit. 'device for making difficulty')). In fact he knew only of ordinary inverters (scramblers). However it was intended to build other types. They were developed by Prof. VIERLING, last known to be at Fauerstein, Franken. He worked with Dr LIEBKNECHT of the Heereswaffenamt. They had developed two types, which he knows about only from conversations with LIEBKNECHT.

31. The first was called 'Baustein'. It too was only an Erschwerungsger"at. It employed two principles: first Ger"auschbeimischung, described as a superimposition of other frequencies on the natural frequencies of the voice stream, and second an inverter. OKW/Chi was not directly concerned with these nor officially told about them. Various people worked on them independently. For example, Siemens worked independently of Vierling and Liebknecht. Baustein was in fact ready recently. He forgets whether the actual production was to have been by Vierling or by Siemens.

32. The second machine was called 'Kuenstliche Sprache' ((artificial speech)). It cut the frequency band vertically into segments and enciphered them separately, in a manner analogous to the encipherment of t/p letters by the SZ 40. He could give no details of the encipherment.

33. He had seen an American machine on the Tigerstedt principle taken from a Mustang. It had a magnetophone band which revolved between nine heads which scrambled the s peech horizontally (i.e. in time). This type of machine was rejected in Germany because you had to wait in between utterances for the machine to act. He himself did not think 750 milliseconds was very long to wait, but he supposed if a German major was talking to a general, the latter would find it desirable to cut him off abruptly with a reply.

34. Asked about the Forschungsamt, he said he knew none of those people until some of them came to Schloss Glucksburg. They had a bad name at OKW/Chi. Nothing was expected from them. He thought they were a big name with nothing behind it. When told that they employed 2,500 people he said, "For their deciphering they should have needed a handful. They must have had other work to do, but what the devil could they have been doing with 2,000 people?"

35. He said that Huttenhains' people had worked on the T52 solutions. He thought that he and Hüttenhain' given sufficient time, and preferably with a captured machine to refer to, could work out the solution for us.

ENCLOSURE TO TICOM/I - 20

TRANSLATION OF FIRST LIST OF ANSWERS.
(actual questionnaire not available).

Nachrichtenstelle Chef WNV Ansacker 18/5/45

Ref. Codes and Cyphers.

In connection with telephone call by
2/Lt. ESCH of 18/5/45.

To: Chief of Defence Force Signals Communications (WNV)

In answer to question 1)

The Dept. responsible for Codes and Cyphers is:

a) For the Army: Within the sphere of Chief of Defence Force Signals Communications (WNV)
b) For the Navy: Within the sphere of Supreme Command of the Navy.
c) For the Air Force: Within the sphere of the C. in C. of the Air Force Southern Sector.

In answer to question 2)

Cyphers for the Army are prepared in approx. 25 printing works in the Central Germany area. They are printed there and are distributed by the Army High Command.
No information can be given as regards cypher preparation and distribution for the Navy and the Air Force.

~~In~~ In answer to question 3)

The senior officer is:

a) For the Army: Lt.Col. METTIG at present at General Eisenhower's G.H.Q.
b) For the Navy: Kapitaen zur See LUCAN Naval supreme Command.
c) For the Air Force: Lt. Col. SCHULZE. - C. in C. of the Air Force Southern Sector.

In answer to question 4)

There are no longer any documents available for the ARmy; orders were issued to destroy them. Nothing is known here on the whereabouts of Naval or Air files.

In answer to question 5)

There is no longer available code or cypher information with Army authorities in the Northern +Sector, as they were destroyed in accordance with orders. No more material is being prepared.
Three trucks of cypher material left HALLE/SAALE in the middle of April to go to the Southern Sector; present whereabouts unknown.
Equipment was administered and distributed for the Army sphere by Army High Command/Signals Dept. (Amtsgruppe Nachrichten). Orders for such equipment were also issued by this authority. Nothing can be said from here, therefore, as to whether equipment is lying in stock anywhere.
Nothing can be said on the above points concerning Air Force or Navy.

In answer to question 6)

As far as we know here, there are no dumps for cypher material for the Army. It is possible that there are still stocks left at the printers of cypher material which has not yet been used.
We know nothing about possible Naval or Air dumps.

TRANSLATION OF SECOND QUESTIONNAIRE.
(Questions 3,4 and 5 and answers only available)

Question 3) Information on all Codes and Cyphers, including cypher machines and books, used by German civil and military authorities in both Germany and the occupied territories and including exhaustive details on their handling.

Answer Information can be given on the following cypher processes (hand and machine cyphers), used by German military and civil authorities in Germany and occupied territories.

I. Hand Cyphers

a) Three letter codes with daily changing recypher by key tables. Three letter codes are books of limited scope, compiled by units themselves within the sphere of the Army and, in the Navy and Air Force, are issued by the Supreme Commands of these parts of the Defence Force. Recyphering tables were all delivered by the Supreme Commands.

b) Raster cypher 44 - Daily changing raster stencils, column and rod keys and conversion tables for encoding the keys. Used by Army, Air Force, Public Authorities; in the Navy only in lateral traffic. In the Army it was also used as a met. key.

c) Raster Replacement cypher and emergency cypher for it. Both are special double transpo. cyphers with squares blacked out in the columns of the first cages. Used by Army, Air Force and Public Authorities.

d) Barbara Code - Figure cards for encoding artillery met. reports for Army and Anti-aircraft artillery. principle of the encoding: Figures of the Barbara tables are added to the figures of the "clear" weather reports.

e) Weather substitution tables - Figure cypher for encyphering met. reports in the Reich Weather Service. Principle of the encyphering: Figures of the clear met. reports are substituted by figures on the met. substitution tables.

f) It is known that other hand keys were in use in the Navy and in the diplomatic service, but details are not known.

II. Machine Cyphers

a) Stecker-Enigma with 3-wheels - Used by Army, Air Force, Public Authorities. Daily changing key: order of wheels, tyre setting, stecker connections. Choice of 3 wheels from a set of 5. To some extent steckered auxiliary wheels are being made.
Changing setting and key from message to message.

b) Stecker-Enigma with 4 wheels - Used by Navy, Daily changing keys as under (a). Choice of 4 wheels from a set of 8. Variable setting and key from message to message.

c) Commercial Enigma - Machine with 4 wheels, no steckers. Used by Public Authorities.

d) Cypher Machine 41 - Hagelin machine with irregularly driven wheels. Used in Reich Meteorological Service as a figure machine. Not used as a letter machine.

III Teleprinter Machines

a) Type 52 c, d, e. - Cypher principle. Substitution and transposition of the impulses of the international T/P alphabet. The changes in the impulses are guided by 10 wheels with fixed lugs. The drive in type 52c is regular but with types 52d and e it is irregular. Daily changing keys. Type 52c used in line working, Types 52d and e in W/T and line working. Used by Army, Navy, Air Force and Public Authorities.

b) Machines 40 and 42. Principle: Substitution of the impulses of the international T/P alphabet directed by 12 wheels with variable lugs. Drive partly regular, partly irregular. Daily changing lugs as keys. Used in line and W/T working. Used by Army and Public Authorities.

c) Teleprinter T 43. Principle: The symbols of the clear teleprint are encyphered by means of individual perforation strips. Used by Army, Navy, and Air Force. Detailed descriptions of the processes and their use are given in the instructions for working. There are no instructions available here.

Question 4) A resume of all call-sign and cover-name systems used by Germany and/or her Allies in W/T and R/T, both in Civil and Military traffic of Germany and the other Allied countries.

Answer I. Call-sign Systems

a) Haphazard choice of call-signs.
Used by Army and Air Force forward of Division. TheSigs Officer responsible at Division chooses call-signs independently.

b) Call-sign Encyphering.
Used by Army and Air Force rearwards of Division. Fixed basic call-signs are issued for lengthy periods in accordance with the Army Call-sign Book. Call-signs are changed by encyphering the basic call-sign with the call-sign key.
The call-sign key itself is a substitution table for figures and letters.
The Enigma machine key serves as an emergency key for encyphering call-signs, whereby the fixed basic call-signs are encyphered.

c) The Naval call-sign systems and those of Public Authorities are not known here.

II. Cover-names and Camouflage devices.

Different cover-names and camouflage tables were issued by the 3 Services which at times were valid for considerable periods. These were not based on definite systems.
In the Army, telephone traffic was camouflaged in accordance with the Army Manual No.427 entitled, "Protection of Signals Communications".
Nothing is known here of the use in the Navy and Air Force of cover-names and camouflage devices.

Question 5) Locations of all W/T, R/T and D/F stations used for enemy signals purposes together with details of their organisation

Answer W/T and R/T traffic were included in:

I. The Wehrmacht Sigint stations at

a) LAUF
b) TREUENBRIETZEN

II. The fixed Army Sigint stations:-

1. (HUSUM)
2. (MUENSTER)
3. (EUSKIRCHEN)
4. (STUTTGART/CANNSTADT)
5. (GRAZ)
6. (TALLN) ? TALLIN
7. (STRIEGAU)
8. (KOENIGSBERG/PR.)

As regards operating and allocation of tasks, the Sigint stations were subordinate to;-

I. Cryptographic office of the Chief of Wehrmacht Signals Communications at OKW;

II. Head Sigint office with Chief of Army Signals matters at OKH.

The results were exploited at:-

I. OKW/Chi,

II. Chief of Army Signals Matters, Head Sigint Office.

Final results were reported to;-

I. OKW. Ops. Staff.

II. General Staff of the Army, foreign armies West or East.

III. There was one D/F station with each of the Wehrmacht - or Fixed Sigint stations.